

There is no circulant weighing matrix of order 60 and weight 36

Abstract

With the help of a computer, we prove the assertion made in the title.

Dragomir Ž. Đoković¹, Ilias S. Kotsireas²

1 Introduction

A *weighing matrix* of order n and weight $w > 0$ is a matrix W of order n whose entries belong to $\{0, \pm 1\}$ such that $WW^T = wI$. (T denotes the transpose and I the identity matrix.) For more information on weighing matrices see [2]. We use the symbol $CW(n, w)$ to refer to a weighing matrix of order n and weight w which is also a circulant. It is well known that if W is a $CW(n, w)$ then $w = a^2$ where a is the sum of the first row of W . The existence question for $CW(60, 36)$ was raised in Strassler's table [5] and has remained open for a long time [1]. We shall prove that $CW(60, 36)$ does not exist.

2 Preliminaries

Let $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z} = \{0, 1, \dots, n-1\}$ be the ring of integers modulo n . Let $A = [a_0, a_1, \dots, a_{n-1}]$ be an integer sequence of length n . We view the indexes $0, 1, \dots, n-1$ as elements of \mathbf{Z}_n . The *periodic autocorrelation function* of A is the real-valued function $\text{PAF}_A : \mathbf{Z}_n \rightarrow \mathbf{R}$ defined by

$$\text{PAF}_A(s) = \sum_{i=0}^{n-1} a_i a_{i+s}. \quad (1)$$

(The indexes should be reduced modulo n .)

Let us now recall some basic facts about a $CW(n, w)$ matrix W . Let $A = [a_0, a_1, \dots, a_{n-1}]$ be its first row and $a = \sum_i a_i$. As mentioned above we have $w = a^2$. By replacing W with $-W$ if necessary, we may assume that $a > 0$. It follows from $WW^T = wI$ that

$$\text{PAF}_A(s) = 0, \quad s = 1, 2, \dots, n-1. \quad (2)$$

By abuse of language, we say that the periodic autocorrelation of A is zero although $\text{PAF}_A(0) = w$ is not zero. The converse is also valid: if A is a ternary sequence (i.e., a sequence with entries

¹University of Waterloo, Department of Pure Mathematics, Waterloo, Ontario, N2L 3G1, Canada e-mail: djokovic@math.uwaterloo.ca

²Wilfrid Laurier University, Department of Physics & Computer Science, Waterloo, Ontario, N2L 3C5, Canada, e-mail: ikotsire@wlu.ca

$0, \pm 1$) of length n and weight w having zero periodic autocorrelation, then the corresponding circulant matrix W is a $CW(n, w)$.

The *discrete Fourier transform* of A is the complex-valued function $\text{DFT}_A : \mathbf{Z}_n \rightarrow \mathbf{C}$ defined by

$$\text{DFT}_A(s) = \sum_{j=0}^{n-1} a_j \omega^{js}, \quad (3)$$

where $\omega = e^{2\pi i/n}$. The *power spectral density* of A is the real-valued function $\text{PSD}_A : \mathbf{Z}_n \rightarrow \mathbf{R}$ defined by

$$\text{PSD}_A(s) = |\text{DFT}_A(s)|^2. \quad (4)$$

We also need the notion of equivalence of integer sequences of fixed length, say n . Denote by X_n the set of such sequences. Let \mathbf{Z}_n^* be the group of units (i.e., invertible elements) of \mathbf{Z}_n . Let Φ_n be the group of affine transformations $\sigma : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$ sending $i \mapsto ui + v$ where $u \in \mathbf{Z}_n^*$, $v \in \mathbf{Z}_n$. The correspondence $\sigma \leftrightarrow \begin{pmatrix} u & v \\ 0 & 1 \end{pmatrix}$ is an isomorphism of Φ_n with the group of these 2×2 matrices over \mathbf{Z}_n . Thus, Φ_n is a semidirect product of \mathbf{Z}_n and \mathbf{Z}_n^* . The action of Φ_n on X_n is defined as follows. If $\sigma \in \Phi_n$ and $x = [x_0, x_1, \dots, x_{n-1}] \in X_n$ then $\sigma(x) = [x_{\sigma^{-1}(0)}, x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n-1)}]$. We say that two sequences in X_n are *equivalent* if they belong to the same orbit of Φ_n .

The basic fact that we need (which is easy to verify) is the following: if a sequence $x \in X_n$ has a zero periodic autocorrelation, then the same is true for any sequence in the equivalence class of x .

Given a factorization $n = md$, we define the *m-compression map* $c_{n,d} : X_n \rightarrow X_d$ as the map sending a sequence $x = [x_0, x_1, \dots, x_{n-1}]$ to the sequence $y = [y_0, y_1, \dots, y_{d-1}]$, where $y_i = x_i + x_{i+d} + \dots + x_{i+(m-1)d}$. It is known that if x has zero periodic autocorrelation, then so does y (see [3]). The reduction map $\mathbf{Z}_n^* \rightarrow \mathbf{Z}_d^*$ modulo d is a surjective group homomorphism, i.e., for each $u \in \mathbf{Z}_d^*$ there exists $\tilde{u} \in \mathbf{Z}_n^*$ such that $\tilde{u} = u \pmod{d}$.

Lemma 1 *Let $\sigma \in \Phi_d$ be given by $\sigma(j) = uj + v$ with $u \in \mathbf{Z}_d^*$, $v \in \mathbf{Z}_d$. Let $\tilde{\sigma} \in \Phi_n$ be given by $\tilde{\sigma}(i) = \tilde{u}i + \tilde{v}$, where $\tilde{u} = u \pmod{d}$ and $\tilde{v} = v \pmod{d}$. Then the following diagram commutes*

$$\begin{array}{ccc} X_n & \xrightarrow{c_{n,d}} & X_d \\ \tilde{\sigma}^{-1} \downarrow & & \downarrow \sigma^{-1} \\ X_n & \xrightarrow{c_{n,d}} & X_d \end{array} \quad (5)$$

Proof Let $x = [x_i]_{i=0}^{n-1} \in X_n$ be arbitrary and let $y = c_{n,d}(x)$, i.e., $y = [y_j]_{j=0}^{d-1} \in X_d$ where $y_j = x_j + x_{j+d} + \dots + x_{j+(m-1)d}$ for $j \in \mathbf{Z}_d$. Let $x' = \tilde{\sigma}^{-1}(x)$ and $y' = \sigma^{-1}(y)$. Thus $x'_i = x_{\tilde{u}i + \tilde{v}}$ for $i \in \mathbf{Z}_n$ and $y'_j = y_{uj+v}$ for $j \in \mathbf{Z}_d$. We have to show that $y' = c_{n,d}(x')$, i.e.,

$$\sum_{k=0}^{m-1} x_{uj+v+kd} = \sum_{k=0}^{m-1} x_{\tilde{u}(j+kd) + \tilde{v}}, \quad j \in \mathbf{Z}_d. \quad (6)$$

Equivalently, we have to show that the two subsets of \mathbf{Z}_n , namely, $\{uj + v + kd : k \in \mathbf{Z}_m\}$ and $\{\tilde{u}j + \tilde{v} + k\tilde{u}d : k \in \mathbf{Z}_m\}$ are equal. As \tilde{u} is relatively prime to n , both subsets are cosets of the additive subgroup of \mathbf{Z}_n generated by d . Since $\tilde{u}j + \tilde{v} = uj + v \pmod{d}$, the two cosets are equal.

3 Main result

We can now prove our main result. Our proof is computational and based on the compression method (see [3]). All computations were performed on the saw.sharcnet.ca cluster running at 2.83 GHz.

Theorem 1 *There is no circulant weighing matrix of order 60 and weight 36.*

Proof For convenience we set $n = 60$ and $w = 36$. Assume that there exists a $CW(n, w)$, say W . Let $A = [a_0, a_1, \dots, a_{n-1}]$ be the first row of W and we set $a = \sum_i a_i$. Let p, q, r denote the number of terms a_i which are equal to $0, 1, -1$, respectively. Since $a^2 = w$ and we can assume that $a > 0$, we have $q - r = a = 6$. As $q + r = w$, we have $p = 24$, $q = 21$, and $r = 15$.

We choose the factorization $n = md$ with $m = 3$ and $d = 20$. By compressing A using the compression factor $m = 3$, we obtain the sequence $B = [b_0, b_1, \dots, b_{d-1}]$ where $b_i = a_i + a_{i+d} + a_{i+2d}$, $0 \leq i < d$. By [3, Theorem 3], B has also periodic autocorrelation zero. Note that each b_i belongs to the set $Z = \{0, \pm 1, \pm 2, \pm 3\}$. For any sequence $[x_0, \dots, x_{d-1}]$ with $x_i \in Z$ we define its *content* to be the sequence $\mu = [\mu_0, \mu_1, \mu_{-1}, \mu_2, \mu_{-2}, \mu_3, \mu_{-3}]$, where μ_j is the number of indexes i such that $x_i = j$. For convenience, we also set $\nu_0 = \mu_0$ and $\nu_i = \mu_i + \mu_{-i}$ for $i = 1, 2, 3$. For a fixed content μ , we denote by X_μ the subset of X_d consisting of all sequences having the content μ . Note that equivalent sequences have the same content, and so X_μ is a union of equivalence classes.

Let μ^B denote the content of B . Let us also set $\nu_0^B = \mu_0^B$ and $\nu_i^B = \mu_i^B + \mu_{-i}^B$ for $i = 1, 2, 3$. Obviously we have $\sum_i \nu_i^B = d$, i.e., the ν_i^B satisfy the equation

$$\nu_0 + \nu_1 + \nu_2 + \nu_3 = 20. \quad (7)$$

Since A has zero periodic autocorrelation, by [3, Theorem 2] we have

$$\text{PSD}_A(s) = w = 36, \quad s = 0, 1, 2, \dots, n-1. \quad (8)$$

By [3, Theorem 3] we also have

$$\text{PSD}_B(s) = w = 36, \quad s = 0, 1, 2, \dots, d-1. \quad (9)$$

By setting $s = 1$ and $\omega_0 = e^{2\pi i/d}$ and by using the fact that B has zero periodic autocorrelation, we obtain that

$$\begin{aligned} \text{PSD}_B(1) &= \left| \sum_{j=0}^{d-1} b_j \omega_0^j \right|^2 = \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} b_j b_k \omega_0^{j-k} \\ &= \sum_{l=0}^{d-1} \left(\sum_{k=0}^{d-1} b_k b_{k+l} \right) \omega_0^l = \sum_{k=0}^{d-1} b_k^2. \end{aligned}$$

Thus $\sum_i i^2 \nu_i^B = w$, i.e., the ν_i^B satisfy the equation

$$\nu_1 + 4\nu_2 + 9\nu_3 = 36. \quad (10)$$

Consequently, μ^B is a nonnegative integral solution of the following system of three linear Diophantine equations:

$$\mu_0 + \mu_1 + \mu_{-1} + \mu_2 + \mu_{-2} + \mu_3 + \mu_{-3} = 20, \quad (11)$$

$$(\mu_1 - \mu_{-1}) + 2(\mu_2 - \mu_{-2}) + 3(\mu_3 - \mu_{-3}) = 6, \quad (12)$$

$$(\mu_1 + \mu_{-1}) + 4(\mu_2 + \mu_{-2}) + 9(\mu_3 + \mu_{-3}) = 36. \quad (13)$$

By a straightforward computer enumeration, we found that there are exactly 76 different contents μ satisfying this system of equations. They are listed in the appendix. Hence, μ^B must be one of these 76 contents. In order to show that the zero autocorrelation property is violated for all sequences in some X_μ , it suffices to do that for the representatives of the equivalence classes contained in X_μ . As a representative of an equivalence class we choose the sequence in the class which is the smallest in the lexicographic ordering. We consider the integers in Z as denoting 7 different colors, and we order them so that $0 < 1 < -1 < 2 < -2 < 3 < -3$. (The above-mentioned lexicographic ordering uses this ordering of the colors.) We refer to these representatives as *charm bracelets* with content μ . An algorithm for generating the charm bracelets of fixed content is presented in the recent preprint [4]. We have applied this algorithm to each of the 76 possible contents μ . The total cpu time used for these computations was about 13 hours and 10 minutes.

The upshot is that altogether there are only four charm bracelets with zero autocorrelation function, namely the following:

$$B_1 = [1, 1, 1, 1, -1, 1, -1, -1, 3, 1, -1, -1, -1, -1, 1, -1, 1, 1, 3, -1],$$

$$B_2 = [0, 0, 0, 0, 0, 0, 0, 0, 3, 3, 0, 0, 0, 0, 0, 0, 0, 0, 3, -3],$$

$$B_3 = [0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 3, 0, 0, 0, 0, 0, 0, 0, 3, 0, -3],$$

$$B_4 = [0, 0, 0, 0, 0, 0, 3, 0, 0, 3, 0, 0, 0, 0, 0, 0, 3, 0, 0, -3].$$

The charm bracelet B_1 has content $[0, 9, 9, 0, 0, 2, 0]$, while B_2, B_3 and B_4 have the same content, namely $[16, 0, 0, 0, 0, 3, 1]$. Thus, B must be equivalent to one of the B_k s, i.e., there exist $\sigma \in \Phi_d$ and $k \in \{1, 2, 3, 4\}$ such that $\sigma^{-1}(B) = B_k$. Say, $\sigma(j) = uj + v$ for all $j \in \mathbf{Z}_d$, where $u \in \mathbf{Z}_d^*$ and $v \in \mathbf{Z}_d$ are fixed. Choose $\tilde{u} \in \mathbf{Z}_n^*$ and $\tilde{v} \in \mathbf{Z}_n$ such that $\tilde{u} = u \pmod{d}$ and $\tilde{v} = v \pmod{d}$. Define $\tilde{\sigma} \in \Phi_n$ by $\tilde{\sigma}(i) = \tilde{u}i + \tilde{v}$. If $A_k = (\tilde{\sigma})^{-1}(A)$ then $c_{n,d}(A_k) = B_k$ by Lemma 1. Thus, by replacing A with A_k we may assume that $B = B_k$.

There are exactly $6^{18} = 101559956668416$ ternary sequences in X_n whose m -compression is B_1 . Also, there are exactly $7^{16} = 33232930569601$ ternary sequences in X_n whose m -compression is B_k , $k = 2, 3, 4$. We have checked with a computer that none of the mentioned ternary sequences has zero periodic autocorrelation. The computation was carried out separately for each of the B_k s. For $k = 1$ we divided the task to 36 processors, so that each processor had to check $6^{16} = 2821109907456$ sequences. The total cpu time used by them was 1144.8 hours. For $k > 1$ we divided the task to 49 processors, so that each processor had to

check $7^{14} = 678223072849$ sequences. The total time used was 383.6, 378.5, 382.0 hours for $k = 2, 3, 4$, respectively.

Since there are no ternary sequences $x \in X_n$ with zero periodic autocorrelation such that $c_{n,d}(x)$ is one of the sequences B_1, B_2, B_3, B_4 , we have a contradiction. Hence, we conclude that there are no $CW(60, 36)$.

4 Acknowledgements

The authors wish to acknowledge generous support by NSERC. This work was made possible by the facilities of the Shared Hierarchical Academic Research Computing Network (SHARCNET) and Compute/Calcul Canada. We also thank Dan Recoskie and Joe Sawada for the use of their code for generating the charm bracelets.

References

- [1] K. T. Arasu and A. J. Gutman, Circulant weighing matrices, *Cryptography and Communications* 2 (2010), 155-171.
- [2] R. Craigen and H. Kharaghani, Orthogonal designs, in *Handbook of Combinatorial Designs*, 2nd ed. C. J. Colbourn, J. H. Dinitz (eds) pp. 280–295. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007.
- [3] D. Ž. Đoković and I. S. Kotsireas, Compression of periodic complementary sequences and applications, *Des. Codes Cryptogr.* DOI 10.1007/s10623-013-9862-z
- [4] D. Ž. Đoković, I. S. Kotsireas, D. Recoskie and J. Sawada, Charm bracelets and their application to the construction of periodic Golay pairs, arXiv:1405.7328 [math.CO]
- [5] Y. Strassler, The classification of circulant weighing matrices with weight 9, PhD thesis, Bar-Ilan University, 1997.

Appendix: The 76 contents μ

We list all 76 nonnegative integral solutions of the system of three linear Diophantine equations (11)-(13).

0, 12, 6, 0, 0, 1, 1	0, 15, 3, 0, 0, 0, 2	0, 9, 9, 0, 0, 2, 0
10, 0, 3, 6, 0, 0, 1	10, 1, 2, 4, 2, 1, 0	10, 2, 1, 5, 1, 0, 1
10, 3, 0, 3, 3, 1, 0	11, 0, 0, 6, 3, 0, 0	11, 0, 5, 1, 0, 3, 0
1, 10, 5, 1, 2, 1, 0	1, 11, 4, 2, 1, 0, 1	11, 2, 3, 0, 1, 3, 0
1, 12, 3, 0, 3, 1, 0	11, 3, 2, 1, 0, 2, 1	1, 13, 2, 1, 2, 0, 1
11, 5, 0, 0, 1, 2, 1	1, 15, 0, 0, 3, 0, 1	12, 0, 2, 4, 0, 1, 1
12, 1, 1, 2, 2, 2, 0	12, 2, 0, 3, 1, 1, 1	14, 0, 1, 2, 0, 2, 1
14, 1, 0, 0, 2, 3, 0	16, 0, 0, 0, 0, 3, 1	1, 6, 9, 3, 0, 1, 0
1, 8, 7, 2, 1, 1, 0	1, 9, 6, 3, 0, 0, 1	2, 11, 1, 2, 4, 0, 0
2, 3, 9, 6, 0, 0, 0	2, 5, 7, 5, 1, 0, 0	2, 7, 5, 4, 2, 0, 0
2, 9, 3, 3, 3, 0, 0	3, 11, 3, 0, 1, 1, 1	3, 12, 2, 1, 0, 0, 2
3, 14, 0, 0, 1, 0, 2	3, 6, 8, 1, 0, 2, 0	3, 8, 6, 0, 1, 2, 0
3, 9, 5, 1, 0, 1, 1	4, 10, 1, 2, 2, 0, 1	4, 11, 0, 0, 4, 1, 0
4, 3, 8, 4, 0, 1, 0	4, 5, 6, 3, 1, 1, 0	4, 6, 5, 4, 0, 0, 1
4, 7, 4, 2, 2, 1, 0	4, 8, 3, 3, 1, 0, 1	4, 9, 2, 1, 3, 1, 0
5, 0, 8, 7, 0, 0, 0	5, 2, 6, 6, 1, 0, 0	5, 4, 4, 5, 2, 0, 0
5, 6, 2, 4, 3, 0, 0	5, 8, 0, 3, 4, 0, 0	6, 10, 0, 0, 2, 1, 1
6, 3, 7, 2, 0, 2, 0	6, 5, 5, 1, 1, 2, 0	6, 6, 4, 2, 0, 1, 1
6, 7, 3, 0, 2, 2, 0	6, 8, 2, 1, 1, 1, 1	6, 9, 1, 2, 0, 0, 2
7, 0, 7, 5, 0, 1, 0	7, 2, 5, 4, 1, 1, 0	7, 3, 4, 5, 0, 0, 1
7, 4, 3, 3, 2, 1, 0	7, 5, 2, 4, 1, 0, 1	7, 6, 1, 2, 3, 1, 0
7, 7, 0, 3, 2, 0, 1	8, 1, 3, 6, 2, 0, 0	8, 3, 1, 5, 3, 0, 0
8, 3, 6, 0, 0, 3, 0	8, 6, 3, 0, 0, 2, 1	8, 9, 0, 0, 0, 1, 2
9, 0, 6, 3, 0, 2, 0	9, 2, 4, 2, 1, 2, 0	9, 3, 3, 3, 0, 1, 1
9, 4, 2, 1, 2, 2, 0	9, 5, 1, 2, 1, 1, 1	9, 6, 0, 0, 3, 2, 0
9, 6, 0, 3, 0, 0, 2		